REMARKS

The subject application is currently under appeal due to the Notice of Appeal filed on December 28, 2004. In conjunction with a Request for Continuing Examination accompanying this Reply, Applicant submits the following remarks in reply to the Official Action of June 29, 2004. The Official Action rejected claims 1-21. Applicant thanks Examiner for examination.

In response, the specification has been amended as indicated above. Claims have been canceled as indicated above. Claims have been added as indicated above. No new matter has been added. Applicant respectfully requests reconsideration in view of the foregoing amendments and these remarks.

Rejections to the Claims under 35 U.S.C. § 102(a)

The Official Action rejected claims 1-21 under 35 U.S.C. § 102(a) as being anticipated by *NIST Special Publication 800-19 – Mobile Agent Security* by Jansen ("Jansen"). Applicant respectfully submits that the new claims traverse the rejections.

Claim 22

New independent claim 22 recites a system including a server that stores a first instance, receives a second instance, and detects unwanted changes between the first and second instances. The server stores the first instance of a mobile application before a jump. The server receives the second instance of the mobile application during the jump. The server detects unwanted changes by comparing the first and second instances.

Jansen generally discloses a survey of security issues associated with mobile software agent technology. Jansen discloses that an agent system addresses some security issues by implementing a client-server architecture. (p. 18-19). Jansen discloses that an agent can modify another agent on a platform if the platform has no control mechanisms in place. (p. 5). Platform modification of agent code can be detected by having an original author digitally sign agent

code. (p. 6-7). However, Jansen teaches that detecting changes to an agent state or data during execution "*does not yet have a general solution.*" (p. 7).

Jansen fails to teach or suggest every limitation of claim 22. Specifically, Jansen fails to teach "*the server storing, prior to a jump to the second host, a first instance of the mobile application.*" Foremost, Jansen only discloses a client-server architecture to address security issues in the abstract, and without proposing how to address the security issues with specific techniques occurring at a server. The claimed server specifically stores a first instance of the mobile application as a snapshot of the mobile application. Jansen wholly fails to contemplate this technique. Thus, Jansen fails to teach or suggest the storing limitation of the server of claim 22.

Jansen also fails to teach "*the server receiving from the first host, during the jump to the second host, a second instance of the mobile application.*" As discussed, Jansen fails to teach or suggest specific server techniques as claimed. The claimed second instance of the mobile application provides a new snapshot of the mobile application at the time of jumping. Jansen is silent with respect to separate instances of the mobile application from different points in time. Thus, Jansen also fails to disclose the receiving limitation of the server of claim 22.

Jansen additionally fails to teach or suggest "*the server detecting unwanted changes in contents of the mobile application including comparing the first and second instances.*" As discussed, Jansen fails to teach or suggest specific server techniques as claimed. The cited alteration detection of Jansen occurs at the platform (e.g., receiving device) and by merely checking a digital signature of an author. Jansen's checking does not compare first and second instances of the mobile application. Thus, Jansen further fails to disclose the detecting limitation of the server module of claim 22 f. Thus, Applicant, respectfully submits that claim 22 is allowable over Jansen.

Claim 28

New independent claim 28 recites a method at a server including the steps of storing a first instance, receiving a second instance, and detecting unwanted changes between the first and

second instances. The first instance is stored prior to a jump. The second instance is received during the jump. Unwanted changes in contents of the mobile application are detected including comparing the first and second instances. Applicant submits that, for at least the same reasons as discussed with respect to claim 22, claim 28 and related dependent claims are allowable over Jansen.

Clam 35

New independent claim 35 recites a computer program product including program instructions tangibly stored on a computer-readable medium and operable to cause a computer system to perform a method at a server including the steps of storing a first instance, receiving a second instance, and detecting unwanted changes between the first and second instances. The first instance is stored prior to a jump. The second instance is received during the jump. Unwanted changes in contents of the mobile application are detected including comparing the first and second instances. Applicant submits that, for at least the same reasons as discussed with respect to claim 22, claim 35 and related dependent claims are allowable over Jansen.

Conclusion

Therefore, Applicant respectfully submits that the presented claims are allowable over Jansen and are in condition for allowance.

Please charge any deficiency in fees or credit any over payment to Deposit Account No. 06-1050.

Applicant : Rygaard et al.
Serial No. : 09/645,028
Filed : August 23, 2000
Page : 10 of 10

Attorney's Docket No.: 18511-005001

Respectfully submitted,

Date: 2/28/05

Dorian Cartwright
Reg. No. 53,853

Fish & Richardson P.C.
500 Arguello Street, Suite 500
Redwood City, California 94063
Telephone: (650) 839-5017
Facsimile: (650) 839-5071

50263281.doc